

REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1, 3-12, 14-17, 19-28 and 30-32 are pending in the application. Claims 1, 12, 17, and 28 are amended by the present amendment. Support for the amended claims can be found in the original specification, claims and drawings.¹ No new matter is presented.

In the Final Office Action of September 21, 2007 (herein, the Final Office Action), Claims 1, 3-11, 16, 19-27 and 32 were rejected under 35 U.S.C. § 103(a) as unpatentable over Hind et al. (U.S. Pat. 6,976,163, herein Hind) in view of Kutaragi et al. (U.S. Pub. 2002/0120722, herein Kutaragi); and Claims 12, 14, 15, 28, 30 and 31 were rejected under 35 U.S.C. § 103(a) as unpatentable over Mattison (U.S. Patent No. 6,615,355) in view of Kutaragi.²

In response to the above noted rejections, Applicants respectfully submit that independent Claims 1, 12, 17 and 28 recite novel features clearly not taught or rendered obvious by the applied references.

Amended independent Claim 1 relates to an image forming apparatus that checks the authenticity of an update program. The apparatus includes a storing unit that stores a program operated by the apparatus and an acquiring unit that acquires an update program from an external source. The apparatus also includes an updating unit that determines whether an electronic signature of the update program is authentic, and updates the program stored in said storing unit using the acquired update program. Independent Claim 1 further recites, in part:

... wherein the authentication of the update program is performed based on a message digest, *the message digest*

¹ E.g., specification, p. 21, lines 7-25.

² Applicants note that Claim 17 was not rejected, but was also not indicated as allowable. Applicants, therefore, request clarification as to the status of pending Claim 17.

being generated based on a configuration file of the update program and a unique identification of the external source.

Independent Claims 1, 12, 17 and 28, while directed to alternative embodiments, recite similar features. Accordingly, the remarks and arguments presented below are applicable to each of amended independent Claims 1, 12, 17 and 28.

As described in an exemplary embodiment at p. 21, ll. 7-25 of the specification, if an SD card is employed as the external source, an electronic signature is generated by generating a message digest based on a cnf (configuration) file and the SD serial ID of the SD memory card. This message digest generated from the cnf file and the SD serial ID is used to determine if the update program is authentic.

In rejecting the previously claimed features directed to the message digest, the Final Office Action relies on col. 3, ll. 1-5; col. 13, ll. 23-35; col. 15, ll. 27-50 and col. 18, ll. 13-60 of Hind. None of these cited portions of Hind, however, teach or suggest that authentication of an update program is performed based on a “***message digest generated based on a configuration file of the update program and a unique identification of the external source,***” as recited in independent Claim 1.

Col. 3, ll. 1-5 of Hind describes a set of rules defining devices for which the application of an update image is authorized. Thus, this cited portion of Hind merely describes the rules defining which devices receive updates and has nothing to do actually authenticating an update program at the device after acquiring the update program, as claimed.

Col. 13, ll. 23-35 of Hind describes that when a customer pays for a particular hardware feature, the customer could receive a license key based on his device serial number, which would allow the customer to reinstall the current standard firmware image release to enable the new feature. Thus, this cited portion of Hind describes what is necessary for a user to receive a firmware update and enable a new feature, but fails to teach or suggest that

an update file is authenticated based on a *message digest generated based on a configuration file of the update program and a unique identification of the external source*, as claimed.

Col. 15, ll. 27-50 of Hind describes that an update image may be accompanied by a digital signature of the image and a certificate chain consisting of one or more X.509 certificates or other suitable certificates. The signature and certificate chain, in combination with a public key of a trusted certificate authority, enable the image recipient to trust the validity of the image, the certificates, and any ancillary data contained in the certificates. Thus, this cited portion of Hind describes that authentication of an image may be performed using the signature, certificate chain, and a key. However, at no point does this cited portion of Hind describe that authentication of the update program is performed based on a *message digest*, much less a message digest *generated based on a configuration file of the update program and a unique identification of the external source*, as claimed.

Col. 18, ll. 13-60 of Hind, along with Figs. 10-11, provide a high-level description of carrying out firmware updates, and lists examples of the authorization needed from the device to be updated so that the proper firmware updates are provided to the appropriate devices. Thus, this cited portion of Hind also fails to disclose authenticating an update program based on a message digest *generated based on a configuration file of the update program and a unique identification of the external source*, as claimed.

Hind, therefore, fails to teach or suggest performing authentication of an update program based on a “*message digest generated based on a configuration file of the update program and a unique identification of the external source*,” as recited in independent Claim 1.

With respect to Claims 12 and 28, the Office Action relies on Mattison instead of Hind in rejecting the claimed features directed to the message digest feature.

Mattison describes a system for providing the protection of flash memory containing a program from any unauthorized programming efforts.³ As described at col. 3, lines 25-33, a flash memory upgrade program containing a new flash memory image would be loaded into system main memory and executed. Then, at col. 3, lines 51-54, Mattison describes a process of comparing an original hash value of the flash memory upgrade program with an independently generated hash value to find a match.

Mattison, however, fails to teach or suggest performing authentication of an update program based on a “*message digest generated based on a configuration file of the update program and a unique identification of the external source*,” as recited in independent Claims 12 and 28.

In rejecting the claimed features directed to the message digest feature, the Final Office Action relies on col. 5, ll. 25-55; col. 8, ll. 1-10; and col. 9, ll. 40-50 of Mattison.

Col. 5, ll. 25-55 of Mattison generally discusses the technique of "hashing," and describes that a hash value is a number that is unique to a block of information so that if any part of the information is modified in that block of information, a subsequently generated hash value will be different. This cited portion of Mattison also describes that a "signature" may be generated for a block of information by a sender generating a hash value using the data in the block of information and then encrypting the generated hash value with the sender's private key. Thus, the encrypted hash value is the signature of the vendor for that block of information.

Mattison, however, fails to teach or suggest teaching creating *a message digest based on a configuration file of the update program and a unique identification of an external source*, and performing authentication of an update program on the basis of this message digest, as claimed. Instead, this cited portion of Mattison merely describes that the process of

³ Mattison, Abstract.

“hashing” exists and that a hash value can be generated to uniquely identify a block of information.

Col. 8, ll. 1-10 and col. 9, ll. 40-50 of Mattison describes that a flash memory upgrade program would incorporate a digital signature which is "signed" by the private key of the vendor; the digital signature being the original hash value of the flash memory upgrade program after the original hash value has been encrypted with the vendor's private key. The source of the update program can then be verified by the recipient of the memory update.

Thus, Mattison describes that the hash value corresponds to the entire flash memory program, not *a configuration file of the update program and a unique identification of the external source*, as claimed. Mattison, therefore, fails to teach or suggest performing authentication of an update program *based on a message digest generated based on a configuration file of the update program and a unique identification of the external source*, as recited in independent Claims 12 and 28.

Further, Kutaragi describes a system enabling mutual exchange of information between users and digital contents, in a manner corresponding to each individual disk. Each optical disk has a unique ID, and the verification server has a user database for accumulating user information corresponding to the disk ID. The verification server identifies the optical disk based on the disk ID, and transmits data corresponding to the optical disk to the computer.

Thus, Kutaragi fails to teach or suggest performing authentication for an update program, much less performing authentication of an update program *based on a message digest generated based on a configuration file of the update program and a unique identification of the external source*, as recited in independent Claims 1, 12, 17 and 28.

Therefore, Hind, Mattison, and Kutaragi, neither alone, nor in combination, teach or suggest the above noted features recited in amended independent Claims 1, 12, 17 and 28.

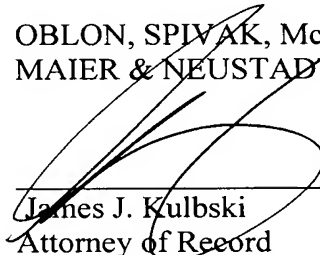
Accordingly, Applicants respectfully request that the rejection of independent Claims 1, 12 and 28 (and the claims that depend therefrom) under 35 U.S.C. § 103 be withdrawn.

Applicants further note that **Claim 17** was not rejected in the Office Action. Nonetheless, Applicants respectfully submit that amended independent Claim 17 also patentably defines over the applied references.

Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1, 3-12, 14-17, 19-28 and 30-32 is patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable consideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



James J. Kulbski
Attorney of Record
Registration No. 34,648

Customer Number

22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

Andrew T. Harry
Registration No. 56,959